AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of 301 W. Parkwood Avenue La Habra, California 90631	)	Case No. 8:24-MJ-00017-DUTY

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: January 18, 2024 at 2:30 p.m.

Karen E. Scott

Judge's signature

City and state: Santa Ana, California

Hon. Karen E. Scott, U.S. Magistrate Judge

Printed name and title

AUSA: M. Rabbani

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
OR07QR24OR0006	01/24/2024 0600	Matthew NAVARRO

Inventory made in the presence of :

SA Sharon Lee

Inventory of the property taken and name of any person(s) seized:

001 Samsung Cell Phone
002 Two handwritten notes

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 03/04/2024

Kevin Leduc

Executing officer's signature

Kevin Leduc Special Agent

Printed name and title

AFFIDAVIT

I, Kevin Leduc, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I have been employed as a Special Agent ("SA") of the United States Department of Homeland Security, Homeland Security Investigations ("HSI") since 2017, and I am currently assigned to the Child Exploitation Investigations Group in Orange County. Prior to my employment as a Special Agent, I was employed as a Computer Forensic Analyst with HSI from 2014-2017. My responsibilities as a SA include investigating crimes involving the sexual exploitation of minors, including, but not limited to, offenses involving travel in foreign commerce to engage in sexually explicit conduct with minors, and offenses involving the production, possession, distribution, and transportation of child pornography.

2. I have completed the Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training at the Federal Law Enforcement Training Center in Brunswick, Georgia. I have also received specific training in the investigation of child exploitation offenses, and I have conducted and participated in numerous child exploitation investigations. As part of these investigations, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18

U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the premises located at 301 W. Parkwood Ave, La Habra, California 90631 (the "SUBJECT PREMISES"), more fully described below and in Attachment A, and to seize evidence, fruits, and instrumentalities of criminal conduct, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of 18 U.S.C. §§ 2251(a), (e) (production of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (collectively, the "Subject Offenses").

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. PREMISES TO BE SEARCHED

5. The SUBJECT PREMISES is the property located at 301 W. Parkwood Ave, La Habra, California 90631. The SUBJECT PREMISES is a single-story dwelling house with a light gray shingle roof and light blue stucco exterior, white trim, and light blue front

door that faces south. The premises has decorative beige and tan stone along the front of the structure. "301" is written in black 4-inch lettering along the white trim above the front door.

IV. DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined in 18 U.S.C. § 2256.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. The term "computer" is defined in 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related

communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. The term "Internet" is defined as the worldwide network of computers — a noncommercial, self-governing network devoted mostly to communication and research with roughly 3.2 billion users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university,

employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

g. The term "Internet Protocol" ("IP") is defined as the primary protocol upon which the Internet is based. IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

h. The term "IP address" is defined as a unique number assigned to each computer directly connected to the Internet (for example, 74.100.66.74). Each computer connected to the Internet is assigned a unique IP address while it is connected. The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that online session.

i. The term "Internet Service Provider" ("ISP") is defined as a business that allows a user to dial into or link through its computers, thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

j. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a

mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

k. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

l. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

V. PROBABLE CAUSE

A. Background on Death of Minor Victim

7. On October 19, 2023, Anaheim Police Department (APD) Detective Sanchez responded to 412 N. Valley St. #1 in the City of Anaheim regarding a possible overdose death (reference Anaheim report #23-157326) of a 16-year-old minor victim ("M.V."). He contacted Officers on the scene and recovered M.V.'s cell phone. M.V.'s grandmother and legal guardian, R.G., signed a consent form allowing a search of the phone, and M.V.'s twin sister, E.G., provided the access code. E.G. informed officers that M.V. had a boyfriend (Matthew Navarro, 21 years

old) who provided M.V. with drugs. Additionally, E.G. was present on October 18, 2023, at around 2230 hours when M.V. snorted Fentanyl before she was found deceased the next morning.

8. M.V.'s cell phone was given to Detective Cunha, who does forensic data extractions for electronic devices within the APD. After the data extraction of M.V.'s cellphone, Detective Cunha provided the extraction to Detective Sanchez, who reviewed M.V.'s cellphone data and saw numerous text messages between Navarro and M.V. indicating they were in a dating relationship. There were several photographs of a sexual nature involving Navarro and M.V. There were several videos showing Navarro having sexual intercourse with M.V. and one video of M.V. performing oral copulation on a male, but the video did not show the male's face. There were numerous photographs of a male's erect penis on the phone, as well as numerous videos of Navarro showing and exposing his penis to the camera on M.V.'s phone.

9. There was a text thread labeled "Amor" in which Navarro sent M.V. a photograph of his face on October 9th at 0036 hours. This photograph matched the other pictures of M.V. and Navarro on her phone. In that same text thread at around 0246 hours, Navarro texted M.V. a video of her performing oral copulation. He then sent two photographs of a hand holding an erect penis with no face in the picture. The two continued to text until Navarro sent a video of him and M.V. having sexual intercourse. He then said, "You have more videos send them plz."

B. Review of Phone Extraction Files

10. On December 04, 2023, I received the files provided on a thumb drive by APD. I viewed all the files and saw that many depicted what appeared to be child sexual abuse material (CSAM). Described below are three of the video files received from APD:

a. The video file titled "IMG_1324.MOV" is approximately one minute and fifty-four seconds in length and depicts M.V. bent over a bed with her feet planted on the ground. M.V. is naked from the waist down, and Navarro is standing behind her with a black shirt on, a gold necklace, and naked from the waist down. M.V. initially is holding the video with the camera facing towards Navarro, who is continuously moving his hips toward her buttocks. Navarro then takes the camera from M.V. and focuses on his penis which is penetrating M.V.'s vagina. Navarro then gives the camera back to M.V., who holds it while he spits down toward their genitals. Navarro takes off the gold necklace and places it around M.V.'s face. Navarro takes his shirt off and then continues to vaginally penetrate M.V. Navarro then takes the camera once again from M.V., where he puts the camera at different angles to capture the sexual intercourse.

b. The Video file titled "IMG_1378.MOV" is approximately thirteen seconds in length and depicts M.V. performing oral copulation on an adult's penis. The adult's face is not visible.

c. The video file titled "IMG_1326.MOV" is approximately forty-eight seconds in length and depicts M.V.

bent over a bed with her feet planted on the floor. M.V. is naked from the waist down, and her unique birthmark on her upper right buttocks is visible. Navarro is seen standing behind her completely naked with his clothes in a pile by his feet. Navarro has an erect penis inserted in M.V.'s vagina from behind. Navarro has possession of the camera and is manipulating it at different angles to capture the sexual intercourse between himself and M.V.

C. Identification of the SUBJECT PREMISES

11. On January 02, 2024, I reviewed California ("CA") Department of Motor Vehicle ("DMV") records for Matthew Navarro California driver's license #Y7240989 with an address listed as the SUBJECT PREMISES. I also reviewed two CA DMV vehicle records for a 2003 silver Dodge Ram (CA plate 30880B2) and a 2005 red Dodge Ram (CA Plate 7T25190) registered to Navarro's family members at the SUBJECT PREMISES.

12. Surveillance was conducted on numerous dates at the SUBJECT PREMISES by Task Force Officer (TFO) George Escanuelas, who witnessed both vehicles parked in the driveway on multiple occasions. I conducted surveillance on January 16, 2024, and witnessed the silver Dodge Ram parked at the SUBJECT PREMISES in the driveway.

D. Characteristics Common to Individuals Who Possess or Intend to View Child Pornography

13. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have

had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have from viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children sometimes possess and maintain "hard copies" of child pornographic material – that is, pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc. When they do, they generally possess these materials in the

privacy and security of their home or some other secure location. When individuals who have a sexual interest in children or images of children collect pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and/or videotapes, they often retain these materials for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children may correspond with and/or meet others to share information and materials; often retain correspondence from other child pornography distributors/ collectors; conceal such correspondence as they do with their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact with and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior

has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

VI. TRAINING AND EXPERIENCE RELATING TO CHILD PORNOGRAPHY AND PERSONS WHO COLLECT CHILD PORNOGRAPHY

14. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that child pornography is readily available on the Internet, from which it can easily be downloaded onto a personal computer, smart phone, or other device with Internet access in the form of digital video and image files. Such digital files are easily saved or copied onto portable electronic data storage devices, such as external hard drives and smaller, more compact thumb and flash drives. Such digital files are also easily copied or "burned" onto CDs and DVDs and transferred onto smart phones and other types of mobile telephones and personal computing devices, such as tablets.

15. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following information about the availability of child pornography on the internet and the practices of persons who distribute, possess, and collect child pornography images and videos:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such

as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, digital photographs, magazines, motion pictures, videotapes, digital videos, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse a selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals may also correspond with others with similar interests to share information and materials. In such cases, these persons rarely destroy correspondence from other child pornography distributors and possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

d. Such individuals frequently also collect and maintain materials evidencing a sexual interest in young children, such as fantasy writings and texts, emails, and chats with other people with similar interests.

e. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, digital videos,

magazines, negatives, photographs, digital photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, digital photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, videotapes and digital videos for many years.

f. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer, an external hard drive, or a flash or thumb drive. Child pornography images stored in this way is often maintained for several years and kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Thus, even if a person suspected of possessing child pornography uses a portable device (such as a mobile phone) to access child pornography on the Internet, there is probable cause, based on my training and experience, to believe that either child pornography or evidence of accessing the Internet with intent to view child pornography will be found in his residence, as well as vehicles located at the person's residence.

g. Some possessors of child pornography have been known repeatedly to download child pornography onto their computers, view it, and then delete it from their computers. In

such cases, evidence of this activity, including deleted child pornography image and video files, often can be located on such person's computers and digital devices using forensic tools.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

16. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such file's months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places

where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

17. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a

complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

18. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Matthew Navarro's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Matthew Navarro's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

19. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

20. For all the reasons described above, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), (e) (production of child pornography), and 2252A(a)(5)(B) (possession of child pornography), as described above and in

//

//

Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachment A of this affidavit.

/s/
Kevin Leduc, Special Agent
Homeland Security
Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 18th day of January 2024.

Karen E. Scott
HONORABLE KAREN E. SCOTT
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

1. The SUBJECT PREMISES is the property located at 301 W. Parkwood Ave, La Habra, California 90631. The SUBJECT PREMISES is a single-story dwelling house with a light gray shingle roof and light blue stucco exterior, white trim, and light blue front door that faces south. The premises has decorative beige and tan stone along the front of the structure. "301" is written in black 4-inch lettering along the white trim above the front door.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violation of 18 U.S.C. §§ 2251(a), (e) (Production of child pornography), and 2252A(a)(5)(B) (possession of child pornography), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8)(A) and (C).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8)(A) and (C), including documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or documents that refer to a transaction of any kind involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or involved in a

transaction of any kind involving child pornography, as defined in 18 U.S.C. § 2256(8)(A) and (C).

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any and all records, documents, programs, applications, materials, or items that are sexually arousing to individuals who are interested in minors, but that are not in and of themselves obscene or that do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques relating to child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of 301 W Parkwood Ave, La Habra, California 90631 (the "SUBJECT PREMISES").

h. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

i. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as

telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic

image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized,

the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending),

including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress Matthew Navarro's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific

finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Matthew Navarro's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.